AB:ADW

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

– X	
	TO BE FILED UNDER SEAL
IN THE MATTER OF AN APPLICATION FOR A SEARCH WARRANT FOR:	AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT
THE PREMISES KNOWN AND DESCRIBED AS 1230 AVENUE Y, APARTMENT C12, BROOKLYN, NEW YORK 11235	No. 19-881 M
– X	

EASTERN DISTRICT OF NEW YORK, SS:

KRISTOPHER SERRA, being duly sworn, deposes and says that he is a Special Agent with the Federal Bureau of Investigation ("FBI"), duly appointed according to law and acting as such.

Upon information and belief, there is probable cause to believe that there is kept and concealed within THE PREMISES KNOWN AND DESCRIBED AS 1230 AVENUE Y, APARTMENT C12, BROOKLYN, NEW YORK 11235 (the "PREMISES"), the items described in Attachment A to this affidavit, all of which constitute evidence or instrumentalities of the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252, 2252A (possession, receipt, and distribution of child pornography — the "Subject Offenses").

The source of your affiant's information and the grounds for his belief are as follows:[1]

1. I have been a Special Agent of the FBI since January 2015, and am currently assigned to the New York Office. Since October 2018, I have been assigned to the Child Exploitation and Human Trafficking Task Force. I have been assigned to investigate violations of criminal law relating to the sexual exploitation of children. I have gained expertise in this area through training in classes and daily work related to conducting these types of investigations. As part of my responsibilities, I have been involved in the investigation of numerous child pornography cases and have reviewed hundreds of thousands of photographs depicting children (less than eighteen years of age) being sexually exploited by adults. Through my experience in these investigations, I have become familiar with methods of determining whether a child is a minor.

2. I have personally participated in the investigation of the offenses discussed below. I am familiar with the facts and circumstances of this investigation from: my own personal participation in the investigation, my review of documents, my training and experience, and discussions I have had with other law enforcement personnel concerning the creation, distribution, and proliferation of child pornography. Additionally, all statements attributable to individuals herein are set forth in sum and substance and in part.

[1] Because this affidavit is submitted for the limited purpose of establishing probable cause for a search warrant, I have not set forth each and every fact learned during the course of the investigation.

3. The FBI is investigating possession, access with intent to view, transportation, receipt, and distribution of sexually explicit material relating to children in violation of Title 18, United States Code, Sections 2252, 2252A (possession, receipt, and distribution of child pornography).

I. DEFINITIONS

4. For the purposes of the requested warrant, the following terms have the indicated meaning in this affidavit:

a. The terms "minor," "sexually explicit conduct" and "visual depiction" are defined as set forth in Title 18, United States Code, Section 2256.

b. The term "child pornography" is defined in Title 18, United States Code, Section 2256(8) in pertinent part as "any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where . . . the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct. . . ."[2]

c. The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, server computers, and network hardware, as well as wireless routers and other hardware involved in network and Internet data transfer.

d. The term "IP Address" or "Internet Protocol Address" means a unique numeric address used by computers on the Internet. An IP address looks like a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP

[2] See also Ashcroft v. Free Speech Coalition, 535 U.S. 234 (2002) (analyzing constitutional validity of the definitions set forth in 18 U.S.C. § 2256(8)).

addresses. Some computers have static — that is, long-term — IP addresses, while other computers have dynamic — that is, frequently changed — IP addresses.

e. The term "Internet" refers to a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

f. The term "storage medium" is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

II. BACKGROUND

5. In or about May 2019, the FBI received information from the National Center for Missing and Exploited Children that approximately 1,700 unique images depicting child pornography had been uploaded to a Yahoo account associated with the name "Manny Colby" and the email address mxc3_inc@yahoo.com (the "SUBJECT ACCOUNT"). Through the use of an administrative subpoena, the FBI determined that the SUBJECT ACCOUNT pertained to the IP address 68.199.10.212 and had accessed the Internet at least 10 times using that IP address between December 2018 and May 2019 via the internet service provider Optimum Online, including on December 16, 2018, February 11, 2019, and May 5, 2019. The FBI further determined that the SUBJECT ACCOUNT accessed the Internet using this IP address through a secure network that would not be accessible to anyone without a password.

6. Law enforcement obtained from Yahoo the approximately 1,700 images that had been uploaded to the SUBJECT ACCOUNT. The following are 3 of those

files that law enforcement obtained from Yahoo. Your affiant reviewed the files downloaded. These files, which are available for the Court's review, are described as follows:

a. File Name: image.1541-2
Description: This is a photograph depicting a nude adult male standing up with an erect penis, as well as a nude prepubescent female standing up with her right hand placed on the adult male's erect penis and her left hand on the adult male's testicles.

b. File Name: image.1591-2
Description: This is a photograph depicting a prepubescent female laying on her stomach while a nude adult male places his hands around the prepubescent female's waist and anally rapes the prepubescent female.

c. File Name: image.196-1
Description: This is a photograph depicting a nude prepubescent female laying on her back, wearing black stockings and silver high heeled shoes, with her knees bent towards her chest while a nude adult male vaginally rapes the prepubescent female.

7. A subpoena to Optimum Online for information regarding the IP address 68.199.10.212 and its accessing of the Internet on December 16, 2018, February 11, 2019, and May 5, 2019 identified the following information:

a. Subscriber: Carlos Castro

b. Address: 1230 Avenue Y, Apartment C12, Brooklyn, NY 11235 (the PREMISES)

c. Phone: (917) 789-9974

8. A search of a public records database was conducted for the PREMISES, identifying the following results:

a. Name: Carlos R. Castro

b. Date of Birth: May 14, 1969

c. SSN: 050-64-0577

9. Based on its investigation to date, the FBI believes that Carlos Castro may be using "Manny Colby" as an alias and using the SUBJECT ACCOUNT. Open source database and website checks indicate that Castro is among the individuals who reside at the PREMISES.

III. CHARACTERISTICS OF COLLECTORS OF CHILD PORNOGRAPHY

10. Based on my training and experience and conversations that I have had with other federal agents and law enforcement officers, I know that child pornography is not readily available in retail establishments. Accordingly, individuals who wish to obtain child pornography do so usually by ordering it from abroad or by discreet contact, including through the use of the Internet, with other individuals who have it available or by accessing web sites containing child pornography. Child pornography collectors often send and receive electronic mail conversing with other collectors in order to solicit and receive child pornography.

11. I know that collectors of child pornography typically retain their materials and related information for many years.

12. I also know that collectors of child pornography often maintain lists of names, addresses, telephone numbers and screen names of individuals with whom they have been in contact and who share the same interests in child pornography.

13. Accordingly, information in support of probable cause in child pornography cases is less likely to be stale because collectors and traders of child pornography are known to store and retain their collections and correspondence with other collectors and distributors for extended periods of time.

14. I also know that child pornography offenders are often recidivists, even while under supervision.

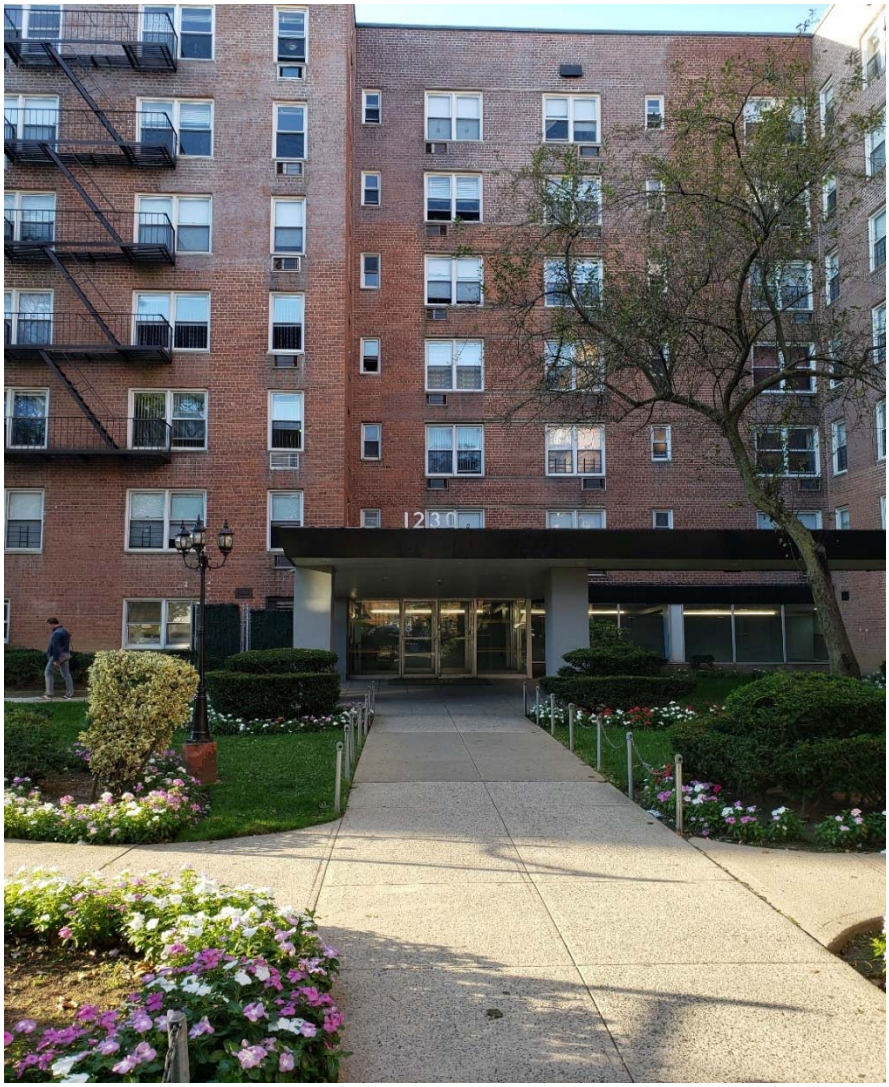
15. Based on my experience, I know that persons who collect and distribute child pornography frequently collect sexually explicit materials in a variety of media, such as photographs, magazines, motion pictures, video tapes, books, slides and/or drawings or other visual media that they use for their own sexual arousal and gratification.

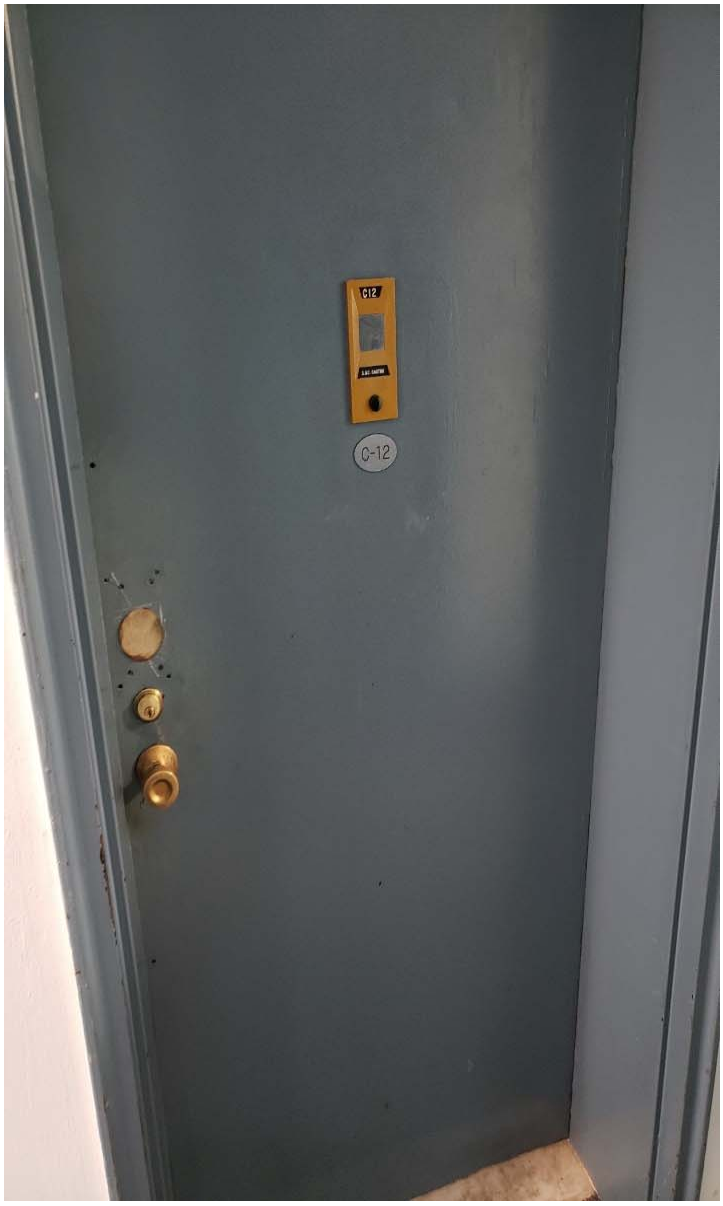
16. Further, based on my training, knowledge, experience, and discussions with other law enforcement officers, I understand that, in the course of executing a search warrant for the possession, transportation, receipt, distribution or reproduction of sexually explicit material related to children, on numerous occasions officers have recovered evidence related to the production of child pornography and/or child exploitation.

IV. THE PREMISES

17. The PREMISES is contained within a multi-story brick building on Avenue Y, between East 12th and East 13th Streets. The entrance to the building is comprised of two sets of glass double doors, one of which is locked. Above the building entrance are the numbers "1230." There is a list of resident names in the lobby of the building. The name "CASTRO, S. & C." is listed next to "C12."

18. The PREMISES is located on the third floor of the building. The door to the PREMISES is grey in color. Affixed to the door is a gold colored door knob, one lock, and a doorbell. "C12" is written in white on a black label above the doorbell, and the name "S. & C. CASTRO" is written in white ink on a black background above the doorbell and below "C12."


1230



V. TECHNICAL BACKGROUND

19. As described above and in Attachment B, this application seeks permission to search for documents constituting evidence, fruits or instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A that might be found on

the PREMISES, in whatever form they are found. One form in which the documents might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of computers and electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B) of the Federal Rules of Criminal Procedure.

20. I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the storage medium that is not currently being used by an active file – for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media – in particular, computers' internal hard drives – contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from the use of an operating system or application, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

21. As further described in Attachment B, this application seeks permission to locate not only electronic computer files that might serve as direct evidence of the crimes described on the warrant, but also electronic "attribution" evidence that establishes how the computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any computer or storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information

such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Forensic evidence on a computer or storage medium can also indicate who has used or controlled the computer or storage medium. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, registry information, Internet search histories, configuration files, user profiles, email, email address books, instant messaging logs, photographs, the presence or absence of malware, and correspondence (and the data associated with the foregoing, such as file creation and last-accessed dates) may be evidence of who used or controlled the computer or storage medium at a relevant time.

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how the computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on a computer is evidence may depend on the context provided by other information stored on the computer and the application of knowledge about how a computer functions. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, it is sometimes necessary to establish that a particular item is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

22. In most cases, a thorough search for information that might be stored on computers and storage media often requires agents to seize such electronic devices and later review the media consistent with the warrant. This is true because of the time required for examination, technical requirements, and the variety of forms of electronic media, as explained below:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on-site. Analyzing electronic data for attribution evidence and conducting a proper forensic examination requires considerable time, and taking that much time on the PREMISES could be unreasonable. Given the ever-expanding data storage capacities of computers and storage media, reviewing such evidence to identify the items described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware

and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the PREMISES. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. The variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

23. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant sought would authorize seizing, imaging, or otherwise copying computers and storage media that reasonably appear to contain some or all of the evidence described in the warrant, and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including, but not limited to, computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

Because several people might share the PREMISES as a residence, it is possible that the PREMISES will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If agents conducting the search nonetheless determine that it is probable that the things described in this warrant could be found on any of those computers or storage media, the warrant sought would permit the seizure and review of those items as well until they are analyzed and cleared for release, at which point they will be returned to their users and/or owners.

VI. CONCLUSION

24. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that on the PREMISES there exists evidence of crimes. Accordingly, a search warrant is requested.

25. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application and search warrant. I believe that sealing these documents is necessary because, given the confidential nature of this investigation, disclosure would severely jeopardize the investigation in that it might alert the target(s) of the investigation at the PREMISES to the existence of an investigation and likely lead to the destruction and concealment of evidence, and/or flight.

WHEREFORE, your affiant respectfully requests that the requested search warrant be issued for THE PREMISES KNOWN AND DESCRIBED AS 1230 AVENUE Y, APARTMENT C12, BROOKLYN, NEW YORK 11235.

IT IS FURTHER REQUESTED that all papers submitted in support of this application, including the application and search warrant, be sealed until further order of the Court.

Special Agent Kristopher Serra
Federal Bureau of Investigation

Sworn to before me this
1st day of October, 2019 by telephone

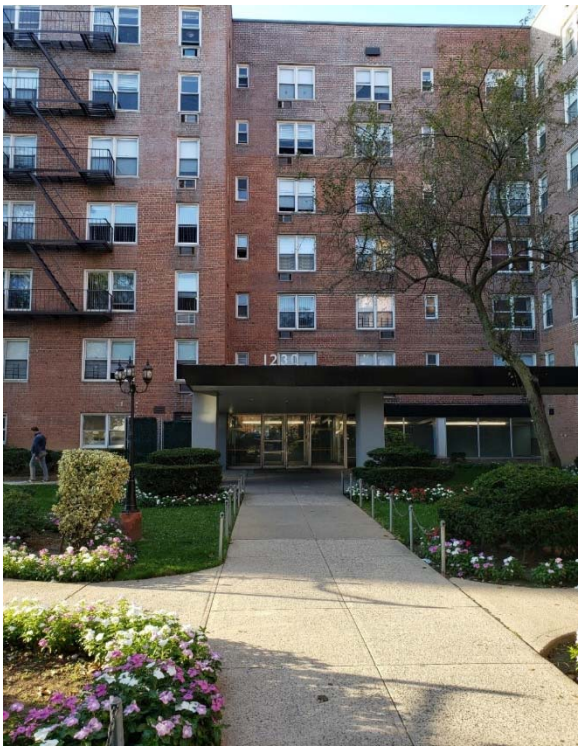
/s/ PK

THE HONORABLE PEGGY KUO
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

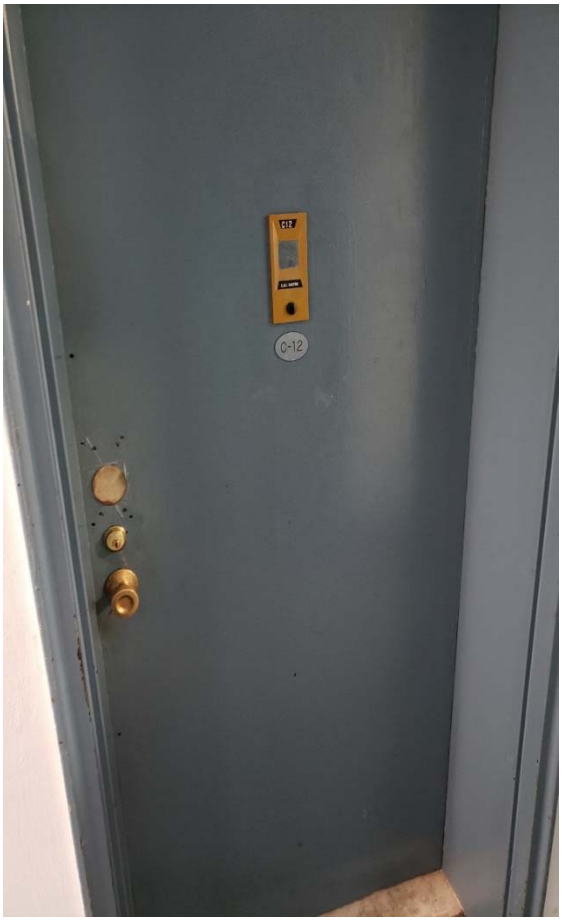
ATTACHMENT A

Property to Be Searched

The property to be searched is 1230 AVENUE Y, APARTMENT C12, BROOKLYN, NEW YORK 11235 (the PREMISES) further described as an apartment contained within a multi-story brick building on Avenue Y, between East 12th and East 13th Streets. The entrance to the building is comprised of two sets of glass double doors, one of which is locked. Above the building entrance are the numbers "1230." There is a list of resident names in the lobby of the building. The name "CASTRO, S. & C." is listed next to "C12." The PREMISES is located on the third floor of the building. The door to the PREMISES is grey in color. Affixed to the door is a gold colored door knob, one lock, and a doorbell. "C12" is written in white on a black label above the doorbell, and the name "S. & C. CASTRO" is written in white ink on a black background above the doorbell and below "C12."




BILLER&JAKOP E 18
BOBOKHODJAEV E 19
BOBROFF,Y. B1
BOCHKNOV,N. F 15
BODENSTEIN,M. D 15
BOGOLANOVS,A&I F 25
BRAYLOVSKIY,L& B 4
BRUSILOVSKY, E 4
BURNOS,Y. D 12
BUTLER, J.&R. E 25
CASTRO, S.&C. C 12
CATANA,D&I. A 16
B 2
CHEHEBAR, M. E 17
CHERNYSHEV, A. 25
CHETVERTKOV,SA C 4
CHOWDHURY, G.&L. F 6
CONSTANTINE,C. B 14
CYNAMON,V. C 5
DE JESUS,T. A 10
DELGADO,B&J. D 2
DESGUIT,S A 19


C-12

ATTACHMENT B

Property to be Seized

ITEMS TO BE SEIZED FROM THE PREMISES, all of which constitute evidence or instrumentalities of violations of Title 18, United States Code Sections 2252 and 2252A:

1. Images of child pornography and files containing images of child pornography and records, images, information or correspondence pertaining to the possession, access with intent to view, receipt and distribution of sexually explicit material relating to children, in violation of Title 18, United States Code, Sections 2252 and 2252A, in any form wherever they may be stored or found;

2. Books and magazines containing visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

3. Originals, copies, and negatives of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256;

4. Motion pictures, films, videos, and other recordings of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

5. Records, information or correspondence pertaining to the possession, access with intent to view, transportation, receipt, distribution and reproduction of sexually explicit material relating to children, as defined in 18 U.S.C. § 2256, including, but not limited to:

    a. envelopes, letters, and other correspondence including, but not limited to, electronic mail, chat logs, and electronic messages, establishing possession, access to, or transmission through interstate or foreign commerce, including by United States mail or by computer, of visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256; and

    b. books, ledgers, and records bearing on the production, reproduction, receipt, shipment, orders, requests, trades, purchases, or transactions of any kind involving the transmission through interstate or foreign commerce including by United States mail or by computer of any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256.

6. Billing and payment records, including records from credit card companies, PayPal and other electronic payment services, reflecting access to websites pertaining to child pornography.

7. Computer-related documentation, meaning any written, recorded, printed, or electronically stored material that explains or illustrates the configuration or use of any seized computer hardware, software, or related items.

8. Records evidencing occupancy or ownership of the PREMISES, including, but not limited to, utility and telephone bills, mail envelopes, or addressed correspondence.

9. Records or other items which evidence ownership or use of computer equipment found in the PREMISES, including, but not limited to, sales receipts, bills for Internet access, and handwritten notes.

10. Address books, mailing lists, supplier lists, mailing address labels and any and all documents and records pertaining to the preparation, purchase and acquisition of names or lists of names to be used in connection with the purchase, sale, trade or transmission of any visual depiction of minors engaged in sexually explicit conduct.

11. Address books, names, lists of names and addresses of individuals believed to be minors.

12. Diaries, notebooks, notes and other records reflecting personal contact and other activities with individuals believed to be minors.

13. Materials and photographs depicting sexual conduct between adults and minors or used in sexual conduct between adults and minors.

14. Any and all records, documents, invoices and materials that concern any Internet accounts used to possess, receive or distribute child pornography.

15. Computers[1] or storage media[2] that contain records or information (hereinafter "COMPUTER") used as a means to commit violations of 18 U.S.C. §§ 2252 and 2252A. All information obtained from such computers or storage media will be maintained by the government for the purpose of authentication and any potential discovery obligations in any related prosecution. The information shall be reviewed by the government only for the purpose of identifying and seizing information that constitutes fruits, evidence and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A including:

a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, instant messaging logs, photographs, and correspondence;

b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

c. evidence of the lack of such malicious software;

d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;

e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;

f. evidence of the times the COMPUTER was used;

g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;

---

[1] A computer includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions, including desktop computers, laptops, mobile phones, tablets, servers, and network hardware, such as wireless routers.

[2] A "storage medium" for purpose of the requested warrant is any physical object upon which computer data can be recorded. Examples include external hard drives, CDs, DVDs and flash drives.

h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER; and

i. contextual information necessary to understand the evidence described in this attachment.

16. Records and things evidencing the use of the Internet Protocol address 69.199.10.212, including:

a. routers, modems, and network equipment used to connect computers to the Internet;

b. Internet Protocol addresses used by the COMPUTER; and

c. records or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

17. During the course of the search, photographs of the searched premises may also be taken to record the condition thereof and/or the location of items therein, all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 2252 and 2252A.